

Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo Pin	Politica de Segurança	1	11/12/2023	MI118

Política de Segurança

Nossa infraestrutura é definida em segurança física e virtual. Nesse documento iremos descrever os critérios utilizados em segurança cibernética.

Infraestrutura física

Sala de TI: A sala da TI é equipada com trava magnética com senha e cartão de acesso autorizados apenas para os funcionários da TI e Diretoria da empresa, possui duas câmeras em sua dependência e alarme que é acionado na empresa de segurança Semprel.

Os racks de são padrões de estrutura fechada e sua chave de acesso possui duas cópias, uma com o gestor do departamento de TI e outra dentro do armário na sala de TI o qual apenas os funcionários de TI possuem as chaves.

Possuimos fisicamente 4 servidores, dois switches gerenciáveis e um firewall, todos dentro de racks.

Existem 3 links de internet para segurança de transmissão e recebimento de dados externos.

Também existem 4 nobreaks que possuem uma autonomia de até 15 min para segurança dos servidores, porém quando o desligamento da energia ocorre em até 5 segundos o gerador é acionado alimentando toda a sala de TI inclusive os nobreaks.

Para refrigeração da sala possuímos dois ar-condicionado, sendo um deles de 30 mil Btus e outro de 20 mil btus como backup.

Segurança do firewall

Nosso firewall é fornecido através da empresa BluePex modelo UTM 3500, sendo configurado e monitorado pela TI e pela BluePex a qual fornece o suporte sempre 24/7.

Em sua configuração possuímos o failover para segurança do link de internet, onde cada link possui uma camada e na falta de um o outro assume de forma automática, garantindo assim a comunicação externa da empresa.

Nosso controle de acesso é configurado através de proxy, vpn e vlan. Garantindo assim a segurança dos colaboradores.

Todo acesso é registrado log e monitorado, criando filtros de permissões de acesso.

Para saber mais detalhes da configuração é apresentando o documento: Firewall UTM 3500.

Por padrão todo acesso é bloqueado através do Proxy, sendo liberado apenas uma lista de colaboradores pré aprovado pela Diretoria.

Para fornecedores externo como Conceitos, Byus, Semprel e colaboradores que trabalham de forma remota, são utilizados acesso via VPN.

Possui link para acesso a internet apenas para visitantes, esse é configurado através da nossa vlan e disponibilizado via wifi com acesso por voucher.

Controle de usuário

Nosso controle de acesso as pastas de rede e ao Windows é tudo autenticado através do nosso AD.

Utilizamos o Domain Controller da Microsoft. Onde definimos OU de acessos, separando por departamento e cada usuário com seu próprio login e senha.

Temos por padrão usuário de acesso comum na fábrica, onde existe um usuário com acesso específico para cada departamento de uso comum, para departamentos administrativos se utiliza um usuário por colaborador.

O acesso é bloqueado por padrão para todos o acesso via Painel de Controle, porta USB, configurado e administrado via GPO.

Os usuários não comuns e não são administradores do Windows.

As pastas de usuário são definidas por grupos e usuários, onde cada um têm acesso apenas ao departamento correspondente.

Para saber mais detalhes da configuração é apresentando o documento: Configurações do AD.